NETWITNESS®

ネットワークフォレンジックツールはネットワークフォレンジックの鍵

ビジネスとテクノロジーの世界は日進月歩であり、この新しいデジタル時代において、ネットワークセキュリティと脅威の検知は、成功する組織のITインフラにとってこれまで以上に重要です。しかし、サイバーセキュリティ対策の強固なシステムがなければ、企業はハッカーやマルウェア、ウイルスなど、悪意のある行為者が仕掛ける攻撃に対して簡単に脆弱になってしまいます。そのため、貴社のような組織は、これらの脅威からネットワークを保護するために積極的なアプローチを取ることが不可欠です。

ネットワークセキュリティ対策というのは、機密データの安全性を確保し、コストのかかる侵害を防ぐだけでなく、サイバー攻撃の潜在的な影響に対する心配を最小限に抑えながら、ビジネス目標の推進に集中することを可能にします。さらに、強固なネットワークセキュリティシステムは、内部と外部の両方の脅威から保護することができるため、ITインフラ全体で安全な環境を維持することが容易になります。しかし、すでに繁栄しているビジネスのオーナーや全国規模の企業であれば、そのようなことはすでにご存知でしょう。

しかし、ネットワークフォレンジックと脅威の検知がどのように機能するかについてはよくご存じないかもしれません。実はここそ、ネットワークフォレンジックツールの出番なのです。そのためNetWitnessでは、ネットワークフォレンジックツールの裏も表も説明し、NetWitnessのエキスパートの働きによってなぜ企業のネットワークが最適に保護されるのか、その理由を説明します。

ネットワークフォレンジックの基本

ネットワークフォレンジックは、デジタルフォレンジックをより詳細に細分化した中の一分野で、ネットワークトラフィックの監視と分析に重点を置いています。この監視プロセスでは、対象のシステムや同じネットワークに接続されている他のデバイスから、ライブでネットワークトラフィックと関連データを収集します。これにより、サイバーセキュリティチームは、マルウェア攻撃、ウイルス、サイバー攻撃などの悪意のある活動を、ビジネスに脅威を与える前に特定することができます。

ネットワークフォレンジックの重要性がわかると、次にネットワークフォレンジックツールが、ネットワークセキュリティの確保を目指す組織にとって必要不可欠なものであることに容易につながります。これらのツールは、不審なユーザーの行動に関する貴重な洞察を提供し、さまざまな外部ソースからの不正アクセスを検知することができます。さらに、サイバーセキュリティインシデントに関連する証拠を収集することで、誰が責任者であったかを発見し、同様のインシデントの再発を防止することができます。

ネットワークフォレンジックツールを使用するメリット

NetWitnessが提供するようなネットワークフォレンジックツールは、企業がネットワークの安全性を確保するための強力で貴重なリソースを提供します。NetWitnessのツールは、ネットワークアクティビティを深く洞察し、トラフィックフローと動作パターンを詳細に可視化します。これにより、企業は疑わしいアクティビティや悪意のある脅威を示す可能性のある異常を迅速に特定できます。また、当社のネットワークフォレンジックツールを使用すると、次のようなことにも気づくでしょう。

ネットワーク全体の可視性が向上

当社のNetWitnessネットワークフォレンジックツールは、企業ネットワークの内部をかつてないほど可視化します。これらのツールは、データトラフィックの収集と分析、使用されている通信プロトコルの特定、悪意のあるアクティビティの検知、パフォーマンス問題のトラブルシューティングをリアルタイムで実行できます。

また、これらの強力で高度な機能を活用することで、企業はネットワーク基盤全体を包括的に把握し、同時に潜在的なセキュリティリスクや脆弱性を特定することができます。

攻撃者に対するセキュリティ態勢を強化

最後になりましたが、当社のネットワークフォレンジックツールは、侵入してくる攻撃者や攻撃者になりそうなものに対する企業のセキュリティ態勢を強化するための強固な安全対策です。ネットワークトラフィックを分析することで、これらのツールは悪意のあるアクティビティを迅速に特定し、攻撃者の行動やその戦術、技術、手順（TTP）に関する詳細な洞察を提供することができます。

また、通信の不審なパターンを検知し、侵害されたデータを発見し、攻撃ベクトルや侵入ポイントに関する情報を明らかにすることができます。しかし、最も重要なことは、ネットワークフォレンジックツールは、攻撃者が悪用できる現在のネットワーク設定の弱点を特定するのにも役立つということです。そして、この知識で武装することで、将来の脅威から組織をよりよく保護するために、防御戦略を調整することができます。

ネットワークフォレンジックツール導入のベストプラクティス

ツール自体はネットワークセキュリティに素晴らしい効果をもたらしますが、ツールを導入する際に留意すべきベストプラクティスがいくつかあります。最も重要なことは、ネットワークフォレンジックツールの導入が、あらゆる角度からネットワークセキュリティを網羅する包括的なアプローチであることを必ず確認してください。

これには、データ・ソース、プロトコル、およびネットワークの徹底的かつ完全な分析に必要なセキュリティ対策を考慮に入れる必要があります。さらに、目標と目的を概説する明確な計画を作成し、明確な期待と手順を設定する必要があります。しかし、ネットワークフォレンジックツールを導入する際、最も重要で、最低限必要なベストプラクティスは次の2つです。

効果的でタイムリーなトレーニングは常に、日々のビジネスオペレーションに新しいテクノロジーを適切に導入する上で最も重要な側面です。そのため、ネットワークフォレンジックツールを実際に使用する社員は、ネットワークフォレンジックツールの適切な使用方法について十分なトレーニングを受けていなければなりません。これは、ツールがその可能性を最大限に活用されることを保証するだけでなく、悪意のある行為者から会社を保護するのにも役立ちます。

選ばれたネットワークセキュリティスタッフは、フォレンジックデータセットからのデータをどのように解釈するか（次のセクションでその理由がわかるでしょう）、また、疑わしいアクティビティや違反を検知するためにツールを使用するためのベストプラクティスに関するトレーニングを受けるべきです。そして、適切なトレーニングによって、貴社のオペレーションは、選択したネットワークフォレンジックツールが効率的かつ安全に使用されることを保証することができます。

不正アクセスからのネットワークデータの保護

ネットワークフォレンジックツールでネットワークを分析し、保護するためにできることは非常に多いため、簡単なことを見落としがちです。そのため、これらのツールを導入するために不可欠なステップは、データが安全に保存され、権限のない人がアクセスできないようにすることです。

貴社のような企業では、すべてのユーザーに認証プロセスを導入し、有線・無線ネットワークに強力な暗号化プロトコルを導入し、機密ファイルやデータへのユーザーアクセスを制限し、ファイアウォール、侵入検知システム、その他の予防技術ソリューションを使用したいと考えるでしょう。また、不審な動きがないか環境全体を定期的に監視することも不可欠なタスクです。侵入を検知した場合に自動で通知やアラートを発することで、攻撃者の一歩先を行くことができます。このような対策を講じることで、企業はネットワークデータを不正アクセスから確実に守ることができます。

大量データの管理

ネットワークフォレンジックツールで作業する際、貴社のような企業が直面するもう一つの主要課題は、生成される可能性のある膨大な量のデータを管理することです。ネットワークフォレンジックツールは、多くの場合、高速で大量のデータを生成します。ご想像の通り、強力な組織的スキルとデータの解釈方法の理解が必要なため、これを管理するのは困難です。

これは、収集したネットワークデータを正確に保存、分析、アーカイブするための手順を用意することで、その量に対応することができます。また、適切な管理方法を整備することで、企業は不審なアクティビティがないかネットワークを容易に監視し、ネットワークフォレンジックツールを簡単に効果的に活用することができます。

NetWitnessを使って貴社のネットワークを安全に

NetWitnessネットワークのセキュリティモニタリングは、絶えず変化するサイバー攻撃の脅威に対して包括的な検知と分析を提供します。このブログで紹介したように、当社のNetWitnessネットワークフォレンジックツールは以下に役立ちます。

- アラートによる疲弊を軽減
- ネットワーク脅威の検知と応答時間を短縮
- 他にもいろいろ！
- 脅威の検知と調査を簡素化
- ネットワークから生成されるすべてのデータを容易に管理・解釈

NetWitnessがあれば、ネットワークは安全で安心でき、疑わしいアクティビティは迅速に特定され、重大な問題に発展する前に対処することができます。ビジネスを保護するための適切なネットワークフォレンジックツールをお探しですか？ それなら、NetWitnessをおいて他にありません！